IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF TEXAS HOUSTON DIVISION

UNITED STATES OF AMERICA	§	
	§	
	§	
v.	§	Criminal Action No: 4:24-cr-00298
	§	
EITHAN DAVID HAIM	§	

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S RENEWED MOTION TO DISMISS

TO THE HONORABLE DAVID HITTNER:

The Government respectfully submits this response in opposition to the defendant's renewed motion to dismiss the Second Superseding Indictment (the "Indictment") (Dkt. 128).

This case involves allegations that the defendant violated a brightline rule in the medical profession—one codified in HIPAA's Privacy Rule[1] and in hospital policies alike: that doctors may not review the medical records of individuals who are not their patients purely out of interest or concern or any personal belief. HIPAA's broadly drafted criminal provision, which provides that doctors cannot

[1] The "Privacy Rule" refers to the regulations promulgated by the Secretary of Health and Human Services at 45 C.F.R. Part 160, and Subparts A and E of Part 164.

obtain individually identifying health information "without authorization," makes such conduct a crime. Whether the defendant obtained the medical records alleged in the Indictment without authorization is a factual question for the jury, not properly considered pretrial. *See United States v. Covington,* 395 U.S. 57, 60 (1969). As set forth below, and for the reasons set forth in the Government's original opposition to the defendant's motion to dismiss (Dkt. 93), the Court should deny the motion.[2]

A. "Without Authorization" Means Without Authorization of the Covered Entity

As the Government previously argued, the meaning of "without authorization" under HIPAA's criminal provision can be determined by straightforward review of the plain language and the context of the statute. (Gov't Opp. at 5-6). *See United States v. Moore*, 71 F.4th 392, 395 (5th Cir. 2023) (statutory interpretation begins with the text of the statute, affording words their ordinary and plain meaning); *United States v. Koutsostamatis,* 956 F.3d 301, 306 (5th Cir. 2020) (emphasizing that the meaning of a statutory phrase should be considered both by its immediate clause and the broader context of the statute as a whole). Within the context of the surrounding terms in the statute, "authorization" refers to the permission of the "covered entity" that

[2] For citation purposes, the defendant's original motion to dismiss (Dkt. 91) is referred to as the "Def. MTD;" the Government original opposition (Dkt. 93) is the "Gov't Opp."; and the defendant's renewed motion to dismiss (Dkt. 128) is the "Def. RMTD."

"maintains" the individually identifiable health information ("IIHI") IIHI. *See* 42 U.S.C. § 1320d-6(a)(2). In this case, the "covered entity" that "maintains" the IIHI is Texas Children's Hospital ("TCH").

The Government's interpretation does not "abandon" the HIPAA Privacy Rule. Rather, the Government is merely suggesting that, for the limited purposes of defining "without authorization" for § 1320d-6, the Court need not look to the Privacy Rule, but can rely on the plain language of the statute. It is the defendant that has abandoned the Privacy Rule, taking the extreme position that the regulations governing all health care providers in the United States are invalid. (Def. RMTD at 5 (noting that the Privacy Rule "binds no one, not even the hospital")).

The defendant argues that the Government's interpretation renders the statute overbroad, allowing hospital policy to impose arbitrary criminal laws, and covering otherwise permissible behavior. (Def. RMTD at 7). But the defendant has not offered a single, *real* example of a situation in which that has happened—only far-fetched hypotheticals. When mounting a facial attack on a statute as overbroad, "the challenger must establish that no set of circumstances exists under which the Act would be valid." *United States v. Salerno*, 481 U.S. 739, 745 (1987) ("[t]he fact that the Bail Reform Act might operate unconstitutionally under some conceivable set of circumstances is insufficient to render it wholly invalid[.]"). The defendant has not

and cannot do so here.

Likewise, his arguments about notice and vagueness fail when considered in context of the allegations in the Indictment. This is not a case where the alleged conduct falls at the fringe of what is legal or illegal. *See United States v. Russell*, No. 23 Cr. 195 (E.D. Va. 2024) (recent criminal case in which defendant was convicted after trial of obtaining IIHI without authorization pursuant to § 1320d-6(a)(2)). As the Government will establish at trial, the defendant had notice that he was not authorized to look at the records of patients he was not treating. Every resident doctor and medical student is trained on that basic precept and the evidence at trial will establish that the defendant was too. Even if there are certain hypothetical scenarios in which an individual might lack notice of what is illegal under § 1320d-6, this is not that case.

1. The Defendant's Proposed Definition of "Without Authorization" Is Unsupported in the Law and Would Render § 1320d-6 Duplicative of the CFAA

The defendant urges the Court to apply a definition of "without authorization" based on the Supreme Court's consideration of an entirely different statute, the Computer Fraud and Abuse Act (the "CFAA"). Essentially, the defendant argues that "authorization" in HIPAA is synonymous with access to the electronic medical records system ("EMR")—either an individual has *access* to the medical records, or he doesn't. The Government previously addressed why the defendant's interpretation

would lead to absurd results vitiating the core privacy concerns that HIPAA was meant to protect; and why *Van Buren* is inapplicable and the CFAA is distinguishable from HIPAA. (Gov't Opp. at 1-10). *See also Bowen v. Porsche Cars, N.A., Inc.*, 561 F. Supp. 3d 1362, 1370, 2021 WL 4726586, at *4 (N.D. Ga. Sept. 20, 2021) (denying motion to dismiss CFAA claim and observing *Van Buren*'s holding on the "exceeds authorized access" prong of CFAA "has no application" to claims brought under the "without authorization prong"); *Speed of Light Ops, LLC v. Elliot*, No. 222CV00246DAKDBP, 2023 WL 2815875, at *3–4 (D. Utah Mar. 21, 2023), *report and recommendation adopted*, No. 2:22CV246-DAK-DBP, 2023 WL 2814604 (D. Utah Apr. 6, 2023) ("Following *Van Buren*, many district courts have recognized that Van Buren's holding applies only to the exceeds authorized access element and did not equally limit the scope of the other provisions of the CFAA, including the without authorization element.") (citing cases).

In the Eastern District of Virginia, a jury recently convicted a defendant of obtaining IIHI without authorization under § 1320d-6 on a similar fact pattern as the one presented here. *United States v. Russell*, No. 23 Cr. 195 (E.D. Va. 2024); *see* "Man Who Illegally Accessed Ginsburg's Records Gets 2 Years in Prison," *New York Times* (Nov. 7, 2024), *available at* https://www.nytimes.com/2024/11/07/us/ruth-bader-ginsburg-medical-records.html. In that case, the defendant, an organ donation

transplant coordinator, accessed the IIHI of Justice Ruth Bader Ginsberg through the EMR system of a hospital. The defendant had access to the EMR system through his job, but he was only supposed to access the medical records for his legitimate job functions. *See id.* Dkt. 78 at 2 (Oct. 31, 2024 Gov't sentencing memorandum). If the Court were to adopt the defendant's proposed definition, the defendant in that case could not have faced criminal consequences for his actions.

In addition to those arguments, the defendant also ignores a significant issue: If the definition of "without authorization" under HIPAA and the CFAA are the same, then HIPAA's criminal provision, which Congress drafted after the CFAA, would be unnecessary and duplicative of the CFAA. *See United States v. Palomares*, 52 F.4th 640, 644 (5th Cir. 2022) (citing *Williams v. Taylor*, 529 U.S. 362, 404 (2000) and recognizing that canon against surplusage gives legal effect to every word and clause in a statute). The CFAA makes it illegal to "intentionally access a computer without authorization . . . and thereby obtain[] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). A "protected computer" under the CFAA can mean "a computer[3] . . . which is used in or affecting interstate or foreign commerce or

[3] A "computer" under the CFAA is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. 1030(e)(1).

communication[.]" 18 U.S.C. 1030(e)(2). There is little question that the EMR systems used by most doctors and hospitals would qualify as a "protective computer" and are in or affecting interstate commerce or communication, given the role they play in health insurance and communications between providers. If "without authorization" under § 1320d-6 is just a "gates up or down" inquiry into whether the defendant had access to an electronic medical record ("EMR") system, as the defendant urges, then § 1320d-6(a) would proscribe exactly the same conduct as the CFAA, and there would have been no need for Congress to pass it as a separate statute.

2. Even Adopting the Defendant's Definition, the Motion to Dismiss Should Still Be Denied

Even if the Court were to adopt the *Van Buren* definition of "without authorization," factual questions would remain such that the Court should deny the motion to dismiss.

The Indictment alleges that the defendant had access to the EMR system not through the ordinary functions of his job, but because he employed false pretenses to get that access—he pretended he needed access for patients under his care, but in reality, he meant only to look at pediatric patients not under his care. (Ind. ¶ 9).[4] In

[4] For purposes of deciding a motion to dismiss, the Court must take the allegations in the Indictment as true. *United States v. Kay*, 359 F.3d 778, 742 (5th Cir. 2004).

other words, the "gates" were up—but only because the defendant impermissibly raised them by false pretenses. The fact that the defendant tricked TCH into giving him access does not equate with authorized access to the system and is more akin to an employee that steals someone else's credentials. *See, e.g.*, *United States v. Willis*, 476 F.3d 1121, 1123, 1125–27 (10th Cir. 2001) (noting that a defendant accesses a computer "without authorization" by falsely posing as someone else and using the login credentials created for the other person to gain access to a protected computer); *United States v. Eddings*, No. 5:19-CR-00535, 2021 WL 2527966, at *4–5 (E.D. Pa. June 21, 2021) ("[T]he mere fact that [Defendant] retained possession of a password which allowed her to access the server post-employment does not, under *Van Buren*, mean that she necessarily was 'authorized' to access the server. Rather, the issue of whether, after she terminated her employment, Denis remained authorized to access the IFC server is properly a question of fact for determination by a jury.").

Moreover, *Van Buren* left open the possibility that even in a "gates-up-or-down" inquiry, whether the gates are up or down might turn on questions of policy. "Although the Supreme Court in *Van Buren* relied on this technical gates-up-or-down inquiry, it left open the issue of 'whether [the authorization] inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies.'" *Moonlight Mountain Recovery, Inc. v. McCoy*,

No. 1:24-CV-00012-BLW, 2024 WL 4027972, at *4 (D. Idaho Sept. 3, 2024) (citing *Van Buren v. United States*, 5933 U.S. 374, 390 n.8 (2021)).

It is a fact question for the jury whether the defendant, in lying to TCH about why he wanted access, was acting with or without authorization. Ultimately, "questions regarding a person's authorized access and the scope of that authorization, as well as the specific information he or she accessed and the location of that information, are fact-intensive inquiries." *Leitner v. Morsovillo*, No. 21-CV-3075-SRB, 2021 WL 2669547, at *4 (W.D. Mo. June 29, 2021). This case raises those factual issues, and the Court should therefore deny the Motion to Dismiss. *See Covington,* 395 U.S. at 60.

B. In the Alternative, the Court Could Interpret "Without Authorization" As Referencing the HIPAA Privacy Rule

The Court could instead choose to interpret "without authorization" as incorporating the HIPAA Privacy Rule, 45 C.F.R. Part 160 and subparts A and E of part 164.[5] The Privacy Rule sets forth when a "covered entity" has authorization to use or disclose IIHI, including an exhaustive set of recognized exceptions when IIHI may be used or disclosed without a patient's authorization. While the Government believes the more straightforward interpretation of "without authorization" is the

[5] Other courts, including the district courts in *United States v. Zhou,* 678 F.3d 1110, 1112-13 (9th Cir. 2012), and *United States v. Russell*, No. 23 Cr. 195 (E.D. Va. 2024) (Dkt. 50), have issued jury instructions based on the Privacy Rule.

argument advanced above, we address this possible interpretation in the alternative. Under either interpretation, the Indictment sets forth a violation of § 1320d-6.

The defendant's original motion to dismiss argues that the Privacy Rule cannot create criminal liability here because (1) the Privacy Rule does not regulate "obtaining" IIHI, only "use or disclosure" (Def. MTD at 19-21); (2) the statutory provision delegating authority to create the regulations that became the Privacy Rule fell outside of the "this part" referenced in § 1320d-6 (*id.* at 21-23); and (3) there are nondelegation concerns in allowing an administrative agency to create regulations subject to criminal penalties (*id.* at 23-24). (Def. MTD at 18-25). These arguments do not withstand scrutiny.

First, while the term "obtain" does not appear in the Privacy Rule, the concept is nevertheless incorporated into the definition of "use." Under the Privacy Rule, "*use* means, with respect to [IIHI], the sharing, employment, application, utilization, *examination*, or *analysis* of such information within an entity that maintains such information." 45 C.F.R. § 160.103 (emphasis added). Webster's Dictionary defines "obtain" as "to gain or attain usually by planned action or effort." Black's Law Dictionary defines "obtain" as "To bring into one's own possession; to procure, esp. through effort." One way to gain, attain, or procure (*i.e.*, obtain) information is by examining it or analyzing it. In other words, under the Privacy Rule, use and obtain

are synonymous.

Second, the words "this part" in § 1320d-6 do not mean Part C of Subchapter XI. Instead, as amended, § 1320d-6 further explains that "a person . . . shall be considered to have obtained or disclosed [IIHI] *in violation of this part* if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation . . .) and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6(a) (emphasis added). *See Robinson v. Shell Oil Co.,* 519 U.S. 337, 341 (1997) (recognizing that statutory language is determined by reference to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole). When read in conjunction with the amendment's language, "in violation of this part" means that (a) the IIHI was maintained by a covered entity; and (b) it was obtained without authorization.

Third, the suggestion that Congress did not incorporate the Privacy Rule into the criminal statute is belied by the text of the statute. Congress added the "without authorization" language to § 1320d-6 *after* the promulgation of the Privacy Rule, and explicitly referenced the "privacy regulation" in the *same sentence* as "without authorization." *See* § 1320d-6(a). Moreover, the word "authorization" is one that appears numerous times in the Privacy Rule in relation to IIHI. *See, e.g.*, 45 C.F.R. 164.508 ("Uses and disclosure for which an authorization is required"); 45 C.F.R.

164.512 ("Uses and disclosures for which an authorization . . . is not required"). Congress's selection of that word in the same sentence as an explicit reference to the Privacy Rule suggests that "without authorization" is an intentional reference to and incorporation of the Privacy Rule.

Fourth, the defendant's stated non-delegation concerns would not render § 1320d-6 unconstitutional under this interpretation. There is no question that Congress delegated authority to HHS to promulgate the regulations at issue, HIPAA § 264(b), 110 Stat. 2033; *South Carolina Medical Ass'n v. Thompson*, 327 F.3d 346 (4th Cir. 2003) (HIPAA did not impermissibly delegate legislative function). The primary case cited by the defendant, *Cargill v. Garland*, 57 F.4th 447 (5th Cir. 2023), addressed a situation in which an administrative agency (the ATF) tasked with enforcing a criminal statute issued regulations interpreting that same statute, *see* 18 U.S.C. § 922(o)(1). Here, the reverse is true: Congress amended § 1320d-6 to explicitly reference and enforce a pre-existing regulatory regime. Section 1320d-6 thus did not delegate authority to HHS, but rather referenced and adopted those regulations that HHS had separately promulgated under Section 264 of HIPAA. And, apart from generalized concerns and a citation to *Cargill*, which was not decided on that basis, the defendant has not pointed to case law in which a criminal statute's reference to regulations was struck down as an unconstitutional delegation of

authority.

In conclusion, under any interpretation of "without authorization"—the one proposed by the Government, the defendant, or one that imports the Privacy Rule as other courts have done—factual issues remain, and the Court should deny the motion to dismiss.

CONCLUSION

WHEREFORE, for the reasons outlined and described above, the Government respectfully requests that Court deny the defendant's renewed motion to dismiss.

Date: December 5, 2024

Respectfully submitted,

ALAMDAR HAMDANI
United States Attorney
Southern District of Texas

By: *s/ Jessica Feinstein*
Jessica Feinstein
Tyler S. White
Assistant United States Attorneys
1000 Louisiana Street, 25th Floor
Houston, Texas 77002
Tel.: (713) 567-9000

CERTIFICATE OF SERVICE

I hereby certify that on December 5, 2024, I electronically filed the foregoing with the Clerk of Court by using the CM/ECF system which will send a notice of electronic filing to all defense counsel of record.

/s/ *Jessica Feinstein*
Jessica Feinstein
Assistant United States Attorney